caBIG™ Security Advisory 103_001:
Potential Vulnerability in the Dorian Identity Provider

A potential vulnerability has been discovered with the Dorian Identity Provider. Complete information on the vulnerability and how to remediate it can be found here: http://www.cagrid.org/wiki/Advisory:2008-07-17:Dorian

This patch has been applied the Dorian Identity Providers on the National Grid. We recommend all users with grid credentials login to the caGrid Portal immediately to upgrade their password: http://cagrid-portal.nci.nih.gov

For Immediate Disclosure

Summary

Title: Digest algorithm used to store passwords in Dorian does not honor all characters
Date: 17-JUL-2008
Product Name: Dorian
OS/Platform(s): All
Reference URL:
http://gforge.nci.nih.gov/tracker/?func=detail&atid=174&aid=15166&group_id=25
Affects: caGrid 1.2 and all prior versions

Description

When Dorian is used as an identity provider, it stores an unrecoverable, 1-way hash (not the actual password), called a digest, in its database.

In a Level of Assurance 1 (LOA1) deployment, Dorian requires that a user's password be 10 characters in length.

A potential vulnerability has been discovered: only the first eight characters are significant, and the last character is used to salt the digest.

Impact

This defect only impacts deployments where Dorian is used as the identity provider.

A user can login successfully using just the first eight and last character (characters 9 - (n-1), where n is the length of the password can be anything).

With respect to Federal eAuthentication guidelines, overall password strength remains level one compliant.

Guessing entropy (the ability to guess one's password) is most affected, the effects on the guessing entropy based on the Federal eAuthentication guidelines are as follows:

- Instead of 32 bits of entropy there are 30 bits of entropy.
- To be LOA2 compliant the system must limit the number of unsuccessful authentication trials.
    - Without the vulnerability the number of unsuccessful tries must be limited to 2^18.
    - With the vulnerability the number of unsuccessful tries must be limited to 2^16.
- With respect to Dorian deployed in the NCI caBIG(TM) national grid:
    - Five, consecutive, invalid logins locks one's account for 4 hours
    - Total invalid logins of 500
    - We do not offer 2^16 (65,536) attempts to guess one's password

Recommended Actions

For Dorian deployments, a patch is available to remediate this defect.

We recommend you download and apply it immediately:

Version	JAR File	Download URL
caGrid 1.2	caGrid-dorian-service-1.2.jar	http://gforge.nci.nih.gov/tracker/download.php/25/174/15166/3715/caGrid-dorian-service-1.2.jar
caGrid 1.1	caGrid-1.1-dorian-service.jar	http://gforge.nci.nih.gov/tracker/download.php/25/174/15166/3724/caGrid-1.1-dorian-service.jar

Instructions

Download the appropriate patch for your version of Dorian. For CCTS, use caGrid 1.1. Overwrite the deployed jar file:

- stop the container Dorian runs in
- copy and overwrite the jar
- start the container

For example: if Dorian has been deployed to Tomcat, the JAR file should be copied to: $CATALINA_HOME/webapps/wsrf/WEB-INF/lib/

Once the patch is applied, users passwords are updated to the new digest the first time they log in.

This patch has already been applied to the Dorian Identity Providers on the National Grid, and we recommend all users with grid credentials login to the caGrid Portal to upgrade their password.

For Additional Support

If you need assistance with this update, we recommend you do one of the following:

- Post your questions to the caGrid_Users-L listserv
- Contact NCICB Application Support: +1-301-451-4384, toll free: +1-888-478-4423, or email: ncicb@pop.nci.nih.gov